Stellungnahme zu den Sicherheitslücken „Meltdown“ und „Spectre“

Retarus stuft Bedrohung für seine Kunden als gering ein

München, 12. Januar 2018 – Aktuell wird in den Medien vermehrt über die hardwareseitigen Sicherheitslücken „Meltdown“ und „Spectre“ diskutiert. Diese Fehler in der Architektur praktisch aller modernen Prozessoren erlauben es, auf eigentlich geschützte Informationen anderer Prozesse auf der gleichen Hardware zuzugreifen. Dies kann im Enterprise-Umfeld insbesondere bei Multimandanten- oder Multi-Purpose-Systemen zu schwerwiegenden Security Breaches führen. Voraussetzung hierfür ist jedoch stets, dass ein Angreifer bereits Code auf den Systemen ausführen kann.

Retarus bietet seine Services im SaaS-Modell (Software-as-a-Service) an. Es gibt dabei keine externen Parteien, die direkt Zugriff auf das nach außen geschlossene System haben. Die Systemhärtung, die eine Code-Einbindung durch Dritte in jeglicher Form verhindert, ist essentieller Bestandteil der gesamten Sicherheitsarchitektur und von unabhängigen externen Sicherheitsexperten getestet. Granularisierung sichert die Retarus-Systeme zusätzlich gegen Angriffe wie „Meltdown“ und „Spectre“ ab. Jedes System erfüllt hierbei möglichst nur eine einzige Funktion. Dank dieser mehrschichtigen Sicherheitsarchitektur stuft Retarus die aktuelle Bedrohung als gering ein.

Um die tiefgehende Security-Separierung weiterhin dauerhaft sicherzustellen, trifft Retarus zusätzliche Vorsichtsmaßnahmen. Für sämtliche eingesetzten Systemkomponenten werden Warnungen und Meldungen des jeweiligen Herstellers genau verfolgt und Handlungsempfehlungen sowie Patches umgehend an den Service-Betrieb weitergegeben. Security Patches werden im Rahmen des Standard- Patch-Managements hinsichtlich Wichtigkeit und Service-Auswirkungen bewertet, getestet und anschließend ausgerollt. Risiken durch bekannte Angriffsvektoren werden so frühzeitig unterbunden. Sollte hierdurch ein Service-Downtime zu erwarten sein, werden die Kunden der Retarus wie gewohnt mit ausreichend Vorlauf informiert. Überdies wird das Intrusion-Detection-and-Prevention-System (IDS/IPS) von Retarus regelmäßig mit bekannten Angriffsmustern trainiert. Damit ließen sich eventuelle Angriffe auf die neuen Prozessor-Schwachstellen frühzeitig erkennen und ggf. blockieren.

Über Retarus

Seit 1992 unterstützt Retarus Unternehmen bei der effizienten und reibungslosen Kommunikation. Der globale Informationslogistiker kommt immer dort ins Spiel, wo große Mengen an Daten sicher und zuverlässig übertragen werden – unabhängig von Kommunikationskanälen, Schnittstellen, Applikationen und Devices. Die Basis hierfür bildet ein Global Delivery Network mit eigenen Rechenzentren in Europa, den USA und der APAC-Region sowie redundanter Carrier-Infrastruktur. Insgesamt vertrauen 75 Prozent der DAX 30 sowie die Hälfte aller EURO STOXX 50 Unternehmen auf Services von Retarus. Zu den langjährigen Kunden zählen unter anderem Adidas, Bayer, Continental, DHL, DZ Bank, Honda, Linde, Osram, Puma, Sixt, Sony und Thomas Cook. Weitere Informationen: www.retarus.de